Dokchitser, T. Y., & Dokchitser, V. (2016). Euler factors determine local Weil representations. Journal für die reine und angewandte Mathematik, 2016(717), 35-46. DOI: 10.1515/crelle-2014-0013

J. reine angew. Math. **717** (2016), 35–46
DOI 10.1515/crelle-2014-0013

Journal für die reine und angewandte Mathematik

Euler factors determine local Weil representations

By *Tim Dokchitser* at Bristol and *Vladimir Dokchitser* at Warwick

Abstract. We show that a Frobenius-semisimple Weil representation over a local field K is determined by its Euler factors over the extensions of K. The construction is explicit, and we illustrate it for l-adic representations attached to elliptic and genus 2 curves. As an application, we construct an absolutely simple 2-dimensional abelian variety over $\mathbb{Q}$ all of whose quadratic twists must have positive rank, according to the Birch–Swinnerton-Dyer conjecture.

1. Introduction

We address the question how to determine an l-adic representation over a local field K from its elementary invariants. For instance, the local Langlands correspondence relies on the characterisation of representations by their local polynomials (i.e. their Euler factors) and 'ϵ-factors of pairs'. The main result of this paper is that they can be recovered just from their local polynomials if one allows extensions of the ground field:

Theorem 1.1. *Every Frobenius-semisimple Weil representation ρ over K is uniquely determined by its local polynomials*

$$P(\rho/F, T) = \det(1 - \mathrm{Frob}_F^{-1}\, T \mid \rho^{I_F}),$$

where F varies over finite separable extensions of K.

The proof of the theorem is explicit, in the sense that it pins down a small number of extensions that suffice.

Many Weil representations arise as restrictions of global representations, e.g. representations of finite Galois groups of number fields (Artin representations) and l-adic Tate modules of elliptic curves and abelian varieties with potentially good reduction. In this case, $P(\rho/K, q^{-s})$ is the local Euler factor of the corresponding global L-function. In the setting of elliptic curves, these local polynomials can be computed using Tate's algorithm over extensions F of K and point counting over the residue fields. The result says that this data suffices to reconstruct $T_l E \otimes \mathbb{Q}_l$ explicitly as a Galois representation.

The first author was supported by a Royal Society University Research Fellowship.

The structure of the paper is as follows. The theorem is proved in Section 2. In Section 3 we give examples how to use the method to describe l-adic representations of elliptic curves. In Section 4 we give a similar example for a genus 2 curve. As an application, we construct an absolutely simple 2-dimensional abelian variety over $\mathbb{Q}$ all of whose quadratic twists must have positive rank, according to the Birch–Swinnerton-Dyer conjecture.

Acknowledgement. The authors would like to thank the University of Sydney, Robinson College (Cambridge) and Emmanuel College (Cambridge), where this research was carried out.

1.1. Notation. Throughout the paper, we use the following notation:

- K is a non-archimedean local field,
- $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, the absolute Galois group of K,
- I_K is the inertia subgroup of G_K,
- Frob_K is an (arithmetic) Frobenius, i.e. any element of G_K acting as $x \mapsto x^{|k|}$ on $\bar{k}$, the algebraic closure of the residue field k of K,
- K^{nr} is the maximal unramified extension of K in K^{sep},
- l is a prime different from the residue characteristic of K,
- μ_n, μ_∞ is the set of n^{th}, respectively all, roots of unity,
- $\mathbf{1}$ is the trivial representation,
- ρ^* is the dual representation of ρ,
- τ is the l-adic tame character $\tau : I_K \to \mathbb{Z}_l$; it maps g to $(\frac{g(\sqrt[l^n]{\pi})}{\sqrt[l^n]{\pi}})_{n\geq 1}$ in $\varprojlim \mu_{l^n} \simeq \mathbb{Z}_l$; here π is any uniformiser of K.

Recall that the Weil group W_K is the subgroup of G_K of all automorphisms that act as an integral power of Frobenius on the residue field, see [13, Section 1.4.1]. It contains the inertia group I_K, and the quotient $W_K/I_K \cong \mathbb{Z}$ is generated by Frob_K.

Recall that a Weil representation is a representation $\rho : W_K \to \mathrm{GL}_n(\mathbb{C})$ whose kernel contains an open subgroup of inertia; in particular, $\rho(I_K)$ is finite. It is called Frobenius-semisimple if the image of some (equivalently, any) Frobenius element is diagonalisable.

The local polynomial $P(\rho, T)$ is the inverse characteristic polynomial of Frob_K^{-1} on the inertia invariants of ρ,

$$P(\rho, T) = \det(1 - \mathrm{Frob}_K^{-1}\, T \mid \rho^{I_K}).$$

Similarly, for a finite extension F/K, we write $P(\rho/F, T)$ for the local polynomial of the restriction of ρ to W_F,

$$P(\rho/F, T) = P(\rho|_{W_F}, T).$$

We will consider l-adic representations, such as τ or the l-adic Tate modules of elliptic curves and abelian varieties; they are known to be Frobenius-semisimple. We fix embeddings

$$\bar{\mathbb{Q}}_l \hookrightarrow \mathbb{C}$$

to convert them into complex representations.

Remark. Recall that a Weil representation ρ is unramified if it satisfies $\rho(I_K) = 1$. Every Frobenius-semisimple unramified representation ρ is completely determined by its local polynomial $P(\rho, T)$. (And, conversely, any polynomial with constant term 1 comes from such a representation.)

2. Local factors determine Weil representations

Theorem 2.1. *Every Frobenius-semisimple Weil representation ρ is uniquely determined by its local polynomials $P(\rho/F, T)$ over finite separable extensions F/K.*

Proof. **Step 1: Cyclic.** Suppose ρ factors through a finite cyclic group

$$G = \mathrm{Gal}(F/K) \cong C_n$$

and the extension F/K has ramification degree e. By Lemma 2.2, there is a cyclic totally ramified extension L/K of degree e such that FL/L is unramified of degree n. The restriction map $\mathrm{Gal}(FL/L) \to \mathrm{Gal}(F/K)$ is an isomorphism, as it is clearly injective and both groups have order n. So ρ/L determines ρ, and ρ/L can be recovered from its local polynomial $P(\rho/L, T)$.

Step 2: Artin to cyclic. Suppose ρ factors through a finite quotient, equivalently it has local polynomial $P(\rho/F, T) = (1-T)^{\dim \rho}$ over some Galois extension F/K. By character theory for the finite group $G = \mathrm{Gal}(F/K)$, it is enough to recover the character of ρ. Thus it suffices to recover the restriction of ρ to every cyclic subgroup $\langle g\rangle < G$ since this gives the value of the character on the conjugacy class of g. This is done in Step 1.

Step 3: Twists. Suppose ρ is a twist of an Artin representation by a 1-dimensional unramified character. Over a sufficiently large Galois extension F/K, we have

$$P(\rho/F, T) = (1-\lambda T)^{\dim \rho}.$$

Let f be the residue degree of the extension F/K and define an unramified character ϕ of W_K by $\mathrm{Frob}_K \mapsto \sqrt[f]{\lambda}$. Then $\rho \otimes \phi^{-1}$ is an Artin representation, and it can be recovered from its local polynomials $P(\rho \otimes \phi^{-1}/L, T) = P(\rho, T/\sqrt[f]{\lambda})$ by Step 2.

Step 4: Weil to Artin. Let ρ be a general Weil representation. By Lemma 2.3, there is a unique decomposition $\rho = \bigoplus_i \rho_i$, such that each summand is a twist of an Artin representation A_i by a 1-dimensional unramified character ψ_i, and the classes of $\psi_i(\mathrm{Frob}_K) \in \mathbb{C}^\times/\mu_\infty$ are distinct. For any F/K,

$$P(\rho/F, T) = \prod_i P(\rho_i/F, T).$$

The roots of the i^{th} factor are those of a given class in $\mathbb{C}^\times/\mu_\infty$ (namely, $[\psi_i(\mathrm{Frob}_K)^{f_{F/K}}]$, where $f_{F/K}$ is the residue degree). By Step 3, this data determines the ρ_i uniquely, and hence ρ as well. □

Lemma 2.2. *Let F/K be a cyclic extension of degree n and ramification degree e. Then there exists a cyclic totally ramified extension L/K of degree e such that FL/L is unramified of degree n.*

Proof. It is enough prove the statement when n is a prime power, since the general case follows immediately by taking the compositum of the corresponding prime-power extensions.

Let χ be a primitive character of $\mathrm{Gal}(F/K)$, and fix a Frobenius element $\mathrm{Frob}_K \in G_K$. We have two cases: If F/K is not totally ramified, pick an unramified character ϕ of G_K of order n with $\phi(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K)^{-1}$. Otherwise, pick any unramified character ϕ of G_K of order n. In either case, let L be the field cut out by $\chi\phi$.

Since $\chi\phi$ is faithful on $I_{F^{\mathrm{nr}}/K}$ and has order $e_{F/K}$, the field L/K is totally ramified of degree e. Moreover, $\chi|_{G_L} = \phi^{-1}|_{G_L}$, so FL/L has degree n, as required. □

Lemma 2.3. *Every Frobenius-semisimple Weil representation over K is a direct sum*

$$\rho = \bigoplus_i A_i \otimes \psi_i,$$

where each A_i factors through a finite quotient, and the ψ_i are 1-dimensional and unramified. There exists such a decomposition such that the classes of $\psi_i(\mathrm{Frob}_K)$ in $\mathbb{C}^\times/\mu_\infty$ are distinct. The latter decomposition is unique in the sense that the components $A_i \otimes \psi_i$ are uniquely determined up to order.

Proof. The first claim is standard: take a sufficiently large finite Galois extension F/K such that ρ/F is unramified. Then $\rho(\mathrm{Frob}_F)$ is central in $\rho(W_K)$, so the eigenspaces of Frob_F are W_K-subrepresentations. Their appropriate unramified twists give the A_i.

Now, if $[\psi_i(\mathrm{Frob}_K)] = [\psi_j(\mathrm{Frob}_K)]$ in $\mathbb{C}^\times/\mu_\infty$, we may replace ψ_j by ψ_i and A_j by $A_j \otimes (\psi_j\psi_i^{-1})$ (which is also an Artin representation) and group the two summands. Repeating this process, we get a decomposition as in the second claim. It is easy to see that it is unique. □

Remark 2.4. There are important local Galois representations that are not Weil representations, e.g. the Tate module of an elliptic curve with multiplicative reduction. These are dealt with by using Weil–Deligne representations $W = (\rho, N)$, where ρ is a Weil representation and N is a nilpotent endomorphism responsible for the 'infinite' part of the inertia group [13]. Their local factors are not sufficient to recover the representation: the local polynomial of W is the same as that of $\ker N$ over any field, so W and $\ker N$ are indistinguishable.

3. Elliptic curve examples

Let E be an elliptic curve defined over a local field K with residue field $k = \mathbb{F}_q$. Consider the l-adic representation associated to E

$$\rho_E : G_K \to \mathrm{GL}_2(\mathbb{C})$$

defined by the Galois action on $H^1_{\text{ét}}(E, \mathbb{Q}_l) \otimes \mathbb{C} = T_l E^* \otimes_{\mathbb{Z}_l} \mathbb{C}$ for any prime $l \neq \mathrm{char}\, k$.

If E/K has good reduction, then ρ_E is unramified by the Néron–Ogg–Shafarevich criterion, so it is completely determined by the characteristic polynomial of $\rho_E(\mathrm{Frob}_K)$. This, in turn, is determined by the number of points on the reduced curve $\tilde{E}/k$,

$$P(\rho_E, T) = 1 - aT + qT^2, \quad a = q + 1 - |\tilde{E}(k)|.$$

If E/K has potentially multiplicative reduction, then it acquires split multiplicative reduction over some separable extension L/K of degree at most 2. The action of G_K on $T_l E$

is described by the theory of the Tate curve ([10, Lemma V.5.2, Excercises 5.11 and 5.13] or [7, Section IV A.1]):

$$\rho_E(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K)\begin{pmatrix}1 & 0\\ 0 & q^{-1}\end{pmatrix}, \quad \rho_E(g) = \chi(g)\begin{pmatrix}1 & \tau(g)\\ 0 & 1\end{pmatrix}, \quad g \in I_K,$$

where $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ is the unique primitive character and τ is the l-adic tame character.

Finally, suppose E/K has additive potentially good reduction. By Theorem 2.1, the l-adic representation ρ_E can be recovered from the local factors $P(\rho_E/F, T)$ over extensions F/K. The proof of the theorem is constructive, and we illustrate it in this section by determining ρ_E for two specific elliptic curves. The idea is to use several fields where E acquires good reduction.

Example 3.1. Consider the elliptic curve

$$E/\mathbb{Q}_{13}\colon\ y^2 = x^3 - 26x.$$

It has additive reduction of type III and acquires good reduction over the field $L = \mathbb{Q}_{13}(\sqrt[4]{13})$, a cyclic quartic totally ramified extension of $\mathbb{Q}_{13}$. So $\rho_E : G_{\mathbb{Q}_{13}} \to \mathrm{GL}_2(\mathbb{C})$ factors through

$$G = \mathrm{Gal}(\mathbb{Q}_{13}^{\mathrm{nr}}(\sqrt[4]{13})/\mathbb{Q}_{13}) \cong \hat{\mathbb{Z}} \times C_4.$$

This group is generated by any Frobenius element $\Phi = \mathrm{Frob}_L$ of G_L and the inertia element g that maps $\sqrt[4]{13}$ to $\iota\sqrt[4]{13}$. (We fix ι to be the fourth root of unity congruent to 5 mod 13.) As G is abelian and Frobenius acts semisimply, ρ_E is diagonalisable. Moreover, g acts faithfully with determinant 1 (by the Weil pairing), so

$$\rho_E(\Phi^{-1}) = \begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}, \quad \rho_E(g) = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$$

for some $\alpha, \beta \in \mathbb{C}$. Counting points of the reduction of E over the residue field $\mathbb{F}_{13}$ of L, we find that $P(\rho_E/L, T) = 1 + 4T + 13T^2$. So $\{\alpha, \beta\} = \{-2 + 3i, -2 - 3i\}$, and it remains to determine which is which.

As in Lemma 2.2, let $L' = \mathbb{Q}_{13}(\sqrt[4]{26})$, so that LL'/L' is quartic unramified. Observe that $\Phi \cdot g$ is a Frobenius element in $G_{L'}$. Indeed, it acts correctly on the residue field, and it fixes $\sqrt[4]{26}$:

$$\begin{aligned}\frac{(\Phi\cdot g)(\sqrt[4]{26})}{\sqrt[4]{26}} &= \frac{\Phi(g(\sqrt[4]{2})g(\sqrt[4]{13}))}{\sqrt[4]{26}}\\ &= \frac{\Phi(\sqrt[4]{2})}{\sqrt[4]{2}}\frac{\Phi(\iota\sqrt[4]{13})}{\sqrt[4]{13}} \equiv (\sqrt[4]{2})^{13-1}\iota \equiv 8\cdot 5 \equiv 1 \mod \pi_{L'}.\end{aligned}$$

As the left-hand side is a fourth root of unity, it must be 1.

Counting points again, we find that

$$P(\rho_E/L', T) = 1 - 6T + 13T^2 = (1 - (3 - 2i)T)(1 - (3 + 2i)T),$$

so that the eigenvalues of $(\Phi\cdot g)^{-1}$ are $3 \pm 2i$. Comparing the eigenvalues of Φ^{-1}, g, $(\Phi\cdot g)^{-1}$, we see that Φ^{-1} must act as $-2 + 3i$ on the i-eigenspace of g, and ρ_E is given by

$$\rho_E(\Phi^{-1}) = \begin{pmatrix}-2 + 3i & 0\\ 0 & -2 - 3i\end{pmatrix}, \quad \rho_E(g) = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}.$$

Example 3.2. Consider the elliptic curve

$$E/\mathbb{Q}_2\colon\ y^2 = x^3 - x.$$

It has additive reduction, and acquires good reduction over $F = \mathbb{Q}_2(E[3])$ ([8, Corollary 2] or [9, Excercise 7.9]). This field is a splitting field of $x^8 - 288x^4 - 6912$ (see [2, Section 3]), equivalently of $x^8 + 6x^4 - 3$. Thus,

$$F = \mathbb{Q}_2(i, \sqrt{3}, \alpha), \quad \alpha = \sqrt[4]{2\sqrt{3} - 3}.$$

Set $z = \frac{\sqrt{3}+i}{2}$, a fixed primitive twelfth root of unity in F, and let β be the fourth root of $-2\sqrt{3} - 3$ given by

$$\beta = (z^2 + z)\alpha.$$

The roots of the polynomial $x^8 + 6x^4 - 3$ in F are $i^k\alpha$ and $i^k\beta$ for $k = 0, 1, 2, 3$. The Galois group $G = \mathrm{Gal}(F/\mathbb{Q}_2)$ is the semi-dihedral group of order 16, and is generated by an 8-cycle and an involution which fixes α,

$$s : \alpha \mapsto -i\beta \mapsto i\alpha \mapsto \beta \mapsto -\alpha \mapsto i\beta \mapsto -i\alpha \mapsto -\beta \mapsto \alpha,$$
$$t : i\alpha \leftrightarrow -i\alpha,\ \beta \leftrightarrow -i\beta,\ -\beta \leftrightarrow i\beta.$$

(In fact, t is complex conjugation in $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong G$.) The inertia subgroup of G is the quaternion group Q_8, generated by s^2 and st.

Fix $\sqrt{-2}$ in $\mathbb{C}$. By [2, Lemma 1],

$$\rho_E \cong A \otimes \eta^{-1},$$

where $\eta : G_{\mathbb{Q}_2} \to \mathbb{C}^\times$ is the unramified character with $\eta(\mathrm{Frob}_{\mathbb{Q}_2}) = \sqrt{-2}$ and A an irreducible 2-dimensional representation of G, which is faithful on the inertia subgroup. Inspecting the character table of G, we see that there are two possibilities for A, called ρ and ρ' in Table 1.

order	1	2	4	8	8	2	4
class	1	s^4	$s^{\pm 2}$	s, s^3	s^5, s^7	$s^{2k}t$	$s^{2k+1}t$
1	1	1	1	1	1	1	1
ϵ_1	1	1	1	1	1	-1	-1
ϵ_2	1	1	1	-1	-1	-1	1
ϵ_3	1	1	1	-1	-1	1	-1
U	2	2	-2	0	0	0	0
ρ	2	-2	0	$-\sqrt{-2}$	$\sqrt{-2}$	0	0
ρ'	2	-2	0	$\sqrt{-2}$	$-\sqrt{-2}$	0	0

Table 1. Character table of G.

As in Step 2 of the proof of Theorem 2.1, to determine what A is we restrict to the (unique) cyclic subgroup of G which distinguishes between ρ and ρ', namely

$$\mathrm{Gal}(F/\mathbb{Q}_2(i)) = \langle s \rangle \cong C_8.$$

Its inertia subgroup is $\langle s^2\rangle \cong C_4$, so $F/\mathbb{Q}_2(i)$ has residue degree 2 and ramification degree 4. As in Step 1 of Theorem 2.1, consider

$$L = \mathbb{Q}_2(i, \sqrt[4]{-3+2i}).$$

It has the property that FL/L is octic unramified. Using e.g. Artin representation machinery in Magma [1], we find that

$$P(\rho/L, T) = 1 + \sqrt{-2}T - T^2, \quad P(\rho'/L, T) = 1 - \sqrt{-2}T - T^2.$$

Moreover, E has good reduction over L, and counting points gives

$$P(\rho_E/L, T) = P(A \otimes \eta^{-1}/L, T) = 1 - 2T + 2T^2.$$

Twisting by η, we get $P(A/L, T) = 1 + \sqrt{-2}T - T^2$, in other words $A = \rho$ and

$$\rho_E \cong \rho \otimes \eta^{-1}.$$

4. A hyperelliptic curve

We illustrate the technique for identifying l-adic representations in the setting of Jacobians of hyperelliptic curves. Their local polynomials, at least when the genus is 2, can be computed from the classification of reduction types and point counting on the reduced curve.

The specific example was chosen to exhibit an absolutely simple abelian variety over $\mathbb{Q}$ all of whose quadratic twists have positive rank, according to the Birch–Swinnerton-Dyer conjecture. Recall that the conjecture says that the Mordell–Weil rank of an abelian variety $A/\mathbb{Q}$ equals the order of vanishing of the L-function $L(A, s)$ at $s = 1$. The L-function is supposed to satisfy a functional equation relating $s \leftrightarrow 2 - s$. Consequently, if the sign in the functional equation is -1, the order of vanishing must be odd, and the rank must be non-zero. This sign is the global root number $w(A/\mathbb{Q})$, and it is defined in terms of the Galois action on the local l-adic representations $H^1_{\text{ét}}(A/\mathbb{Q}_p, \mathbb{Q}_l)$ for each p. We will construct an absolutely simple abelian variety $J/\mathbb{Q}$ whose global root number, and that of each of its quadratic twists, is -1. Such examples are impossible for elliptic curves over $\mathbb{Q}$, but do exist for elliptic curves over number fields [3]. The question of existence of such abelian varieties over $\mathbb{Q}$ was posed to us by V. Flynn.

Example 4.1. Consider the genus 2 curve

$$C/\mathbb{Q}\colon\ y^2 + y = x^5 - 11x^4 - 6x^3 + 9x^2 + x - 1,$$

and let $J/\mathbb{Q}$ be its Jacobian. For a prime p, let $\rho_J = \rho_{J,p} : G_{\mathbb{Q}_p} \to \mathrm{GL}_4(\mathbb{C})$ be the Galois representation on

$$H^1_{\text{ét}}(C/\mathbb{Q}_p, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \mathbb{C} \cong H^1_{\text{ét}}(J/\mathbb{Q}_p, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \mathbb{C} \cong (T_l J)^* \otimes_{\mathbb{Z}_l} \mathbb{C} \quad (l \neq p).$$

We will show that

(a) J has bad reduction only at 13 and 2633.

(b) J is absolutely simple.

(c) At $p = 2633$ the representation $\rho_J = \rho_{J,p}$ is, in a suitable basis,

$$\rho_J(\mathrm{Frob}_{\mathbb{Q}_p}^{-1}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}, \quad \rho_J(g) = \begin{pmatrix} 1 & 0 & \tau(g) & 0 \\ 0 & 1 & 0 & \tau(g) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

for all $g \in I_{\mathbb{Q}_p}$, where τ is the l-adic tame character.

(d) At $p = 13$ the representation $\rho_J = \rho_{J,p}$ factors through

$$G = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}(\sqrt[4]{13})/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times C_4.$$

This group is generated by any Frobenius element Φ of $G_{\mathbb{Q}_p(\sqrt[4]{13})}$ and the inertia element g that maps $\sqrt[4]{13}$ to $\iota\sqrt[4]{13}$. (We fix ι to be the fourth root of unity congruent to 5 mod 13.) In a suitable basis,

$$\rho_J(\Phi^{-1}) = \begin{pmatrix} -2-3i & 0 & 0 & 0 \\ 0 & -2+3i & 0 & 0 \\ 0 & 0 & -2-3i & 0 \\ 0 & 0 & 0 & -2+3i \end{pmatrix}, \quad \rho_J(g) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}.$$

(e) The root number of every quadratic twist of the Jacobian $J/\mathbb{Q}$ is -1. Assuming the Birch–Swinnerton-Dyer conjecture for abelian varieties, every quadratic twist of J has positive Mordell–Weil rank.

Proof. (a) Using Magma [1] and Sage [11], we find that the curve C has discriminant $13^3 \cdot 2633^2$ and reduction types I_0-III-0 at 13, and $\mathrm{I}_{1\text{-}1\text{-}0}$ at 2633 in the Namikawa–Ueno classification [5].

(b) Stoll ([12, Lemma 3]) gives an explicit criterion for J to be absolutely irreducible: it suffices to find a prime p of good reduction such that the local factor $f(T) = P(\rho_{J,p}, T)$ is irreducible, and such that the modified resultant $\mathrm{Res}_T(f(T), f(Tx))/(x-1)^{2\dim J}$ has no irreducible monic factors in $\mathbb{Z}[x]$ of constant term 1. Counting points over $\mathbb{F}_{3^n}$, we find that for $p = 3$,

$$P(\rho_{J,p}, T) = 1 - T + 2T^2 - 3T^3 + 9T^4,$$

which is irreducible, and

$$\frac{\mathrm{Res}_T(f(T), f(Tx))}{(x-1)^4} = 3^8\left(x^4 + \frac{4}{3}x^3 + x^2 + \frac{4}{3}x + 1\right)^2\left(x^4 + x^3 + \frac{16}{9}x^2 + x + 1\right),$$

fulfilling the criterion.

(c) Analysis at $p = 2633$: Either checking by bare hands or by using the classification of reduction types, we see that the equation for C defines a regular model at p. The reduced curve is

$$\tilde{C}\colon\ y^2 = (x-2344)^2(x-645)^2(x-1952),$$

so the special fibre is a $\mathbb{P}^1$ with two self-intersections. The slopes at both singular points are $\mathbb{F}_p$-rational, so $\tilde{C}$ has $q + 1 - 2$ points over any extension $\mathbb{F}_q/\mathbb{F}_p$. The local polynomial is therefore

$$P(C/\mathbb{Q}_p, T) = (1-T)^2.$$

In particular, the invariant subspace $\rho_{J,p}^{I_p}$ is 2-dimensional, with trivial action of Frobenius. The action of the inertia group on the whole space is described in Namikawa–Ueno [5, p. 179], and the action of Frobenius is forced by its action on inertia invariants and the relation

$$\mathrm{Frob}_{\mathbb{Q}_p}\, g\, \mathrm{Frob}_{\mathbb{Q}_p}^{-1} = g^p$$

for g in the tame inertia quotient.

(d) Analysis at $p = 13$. The reduced curve is

$$\tilde{C}\colon\ y^2 = (x+2)^3(x^2+9x+6),$$

and its normalisation is an elliptic curve

$$(\dagger) \qquad E_1/\mathbb{F}_{13}\colon\ y^2 = (x+2)(x^2+9x+6).$$

From the Namikawa–Ueno classification [5, p. 161],

$$\rho_{J,13} = \rho_{J,13}^{I_{13}} \oplus W$$

with 2-dimensional summands, as an I_{13}-representation. Moreover, inertia acts on W as $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, that is through the cyclic tame quotient of order 4. Since the inertia subgroup is normal, the action of Frobenius necessarily preserves this decomposition. Using Magma [1], we find

$$P(\rho_{J,13}, T) = 1 + 4T + 13T^2,$$

which describes the action of $G_{\mathbb{Q}_{13}}$ on the inertia invariant subspace $\rho_{J,13}^{I_{13}}$:

$$\Phi^{-1} \mapsto \begin{pmatrix} -2-3i & 0 \\ 0 & -2+3i \end{pmatrix}, \quad g \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ for } g \in I_{13}.$$

Next, we reconstruct the Galois action on the whole space from the local polynomials over suitable extensions of $\mathbb{Q}_{13}$. Consider $L = \mathbb{Q}_{13}(\sqrt[4]{13})$ and $L' = \mathbb{Q}_{13}(\sqrt[4]{26})$. Over both fields the curve C has reduction of type I_0-I_0-1, its Jacobian has good reduction, and the special fibre of C is two elliptic curves meeting at a point. One of these elliptic curves over L and over L' is the same curve E_1 as above. The other one is, respectively,

$$E_2\colon\ y^2 = x^3 - 5x, \quad E_2'\colon\ y^2 = x^3 - x.$$

Their local polynomials are

$$\begin{aligned} P(E_1/\mathbb{F}_{13}, T) &= 1 + 4T + 13T^2, \\ P(E_2/\mathbb{F}_{13}, T) &= 1 + 4T + 13T^2, \\ P(E_2'/\mathbb{F}_{13}, T) &= 1 - 6T + 13T^2. \end{aligned}$$

By counting points of $\tilde{C}$, E_1, E_2 and E_2' over $\mathbb{F}_{13^n}$, considering the corresponding ζ-functions and computing H^0 and H^2 of the special fibres, we find

$$\begin{aligned} P(\rho_{J,13}/L, T) &= (1 + 4T + 13T^2)^2, \\ P(\rho_{J,13}/L', T) &= (1 + 4T + 13T^2)(1 - 6T + 13T^2). \end{aligned}$$

Therefore the eigenvalues on W of g, $\mathrm{Frob}_L^{-1}(=\Phi^{-1})$ and $\mathrm{Frob}_{L'}^{-1}$ are, respectively,

$$\{i,-i\},\quad \{-2-3i,-2+3i\},\quad \{3-2i,3+2i\}.$$

Exactly as in the end of Example 3.1, it follows that Φ^{-1} must act as $-2+3i$ on the i-eigenspace of g on W and as $-2-3i$ on the $(-i)$-eigenspace. This completes the description of $\rho_{J,13}$.

(e) Let $\chi : G_{\mathbb{Q}} \to \pm 1$ be a character of order 1 or 2, and let J_χ be the quadratic twist of J by χ. Thus J_χ is the Jacobian of

$$C_d\colon\ dy^2 = x^5 - 11x^4 - 6x^3 + 9x^2 + x - \frac{3}{4},$$

where $\mathbb{Q}(\sqrt{d})$ is the field cut out by χ. As a $G_{\mathbb{Q}}$-representation $T_l J_\chi \cong T_l J \otimes \chi$, and

$$\rho_{J_\chi,p} \cong \rho_{J,p} \otimes \chi$$

for every prime p. The global root number $w(J_\chi/\mathbb{Q})$ is, by definition, the product of local root numbers $w_v(J_\chi) = w(J_\chi/\mathbb{Q}_v)$ over all places of $\mathbb{Q}$,

$$w(J_\chi) = \prod_v w_v(J_\chi).$$

The local root number is the 'sign' of the local ϵ-factor,

$$w_v(J_\chi) = \frac{\epsilon_v(J_\chi,\psi,\mu)}{|\epsilon_v(J_\chi,\psi,\mu)|},$$

and we refer to Tate [13] for the definition and basic properties of local ϵ-factors; see also [4, Appendix A].

We claim that, independently of χ,

$$w_v(J_\chi) = \begin{cases} -1 & \text{if } v = 13,\\ +1 & \text{otherwise,}\end{cases}$$

so the global root number of any quadratic twist of J is -1, as required.

For $v=\infty$, the local root number is defined in terms of the Hodge structure of J_χ, and for an abelian variety $A/\mathbb{Q}$ it is simply $(-1)^{\dim A}$; see e.g. [6, Lemma 2.1]. In our case $\dim J_\chi = 2$ and $w_v(J_\chi) = +1$.

At all primes $v \neq 13$, the abelian variety J is semistable, and the root number computation is standard: see e.g. [4, Proposition 3.23] with $\tau = \chi$ and $X(\mathcal{T}^*) = \mathbf{1}\oplus\mathbf{1}$ for $v = 2263$ and 0 else; note also that $w(\chi)^4 = 1$ by Lemma 4.2 (1).

At $v = 13$, the representation $\rho_{J,13}$ is described above in (d). Observe that

$$\rho_{J,13} \cong \rho_{E,13} \oplus \rho_{E',13},$$

where E is the curve (†) lifted to $\mathbb{Q}_{13}$,

$$E\colon\ y^2 = (x+2)(x^2+9x+6),$$

and E' is the curve in Example 3.1,

$$E'\colon\ y^2 = x^3 - 26x.$$

The first one has good reduction, and the second one has additive reduction of type III. In the terminology of [3], E is 'lawful good' and E' is 'lawful evil' (see [3, Classification 3]). In other words, the local root numbers are $w(E) = +1$, $w(E') = -1$ and $w(E/F) = w(E'/F) = 1$ for every quadratic extension $F/\mathbb{Q}_{13}$. Now, if $\chi = \mathbf{1}$, then

$$w_{13}(J \otimes \chi) = w(\rho_{J,13}) = w(\rho_{E,13})w(\rho_{E',13}) = w(E)w(E') = -1.$$

If χ has order 2 and F is the field cut out by χ, then by Lemma 4.2 (2),

$$w_{13}(J \otimes \chi) = w(E \otimes \chi)w(E' \otimes \chi) = \frac{w(E/F)}{w(E)\chi(-1)}\frac{w(E'/F)}{w(E')\chi(-1)} = -1.$$

This completes the proof. □

Lemma 4.2. *Let K be a local field and let $\chi : G_K \to \pm 1$ be a character of order ≤ 2.*

(1) *We have $w(\chi)^2 = \chi(-1) = \pm 1$, where $\chi(-1)$ denotes χ evaluated on the image of -1 under the local reciprocity map $K^\times \to G_K^{\mathrm{ab}}$.*

(2) *Suppose $\chi \neq \mathbf{1}$ and let F/K be the quadratic extension cut out by χ. For a Weil representation V/K of even dimension $2g$,*

$$w(V)w(V \otimes \chi) = w(V/F)\chi(-1)^g.$$

Proof. (1) By the determinant formula [13, formula (3.4.7)],

$$w(\chi)^2 = w(\chi \oplus \bar{\chi}) = \chi(-1).$$

(2) Write Ind for the induction of representations from G_F to G_K. By inductivity of root numbers in degree 0,

$$\begin{aligned} w(V)w(V \otimes \chi) &= w(\operatorname{Ind} V/F) \\ &= w(\operatorname{Ind}(V \ominus \mathbf{1}^{\oplus 2g}/F))w(\operatorname{Ind}\mathbf{1}^{\oplus 2g}) \\ &= \frac{w(V/F)}{w(\mathbf{1}/F)^{2g}} w(\mathbf{1})^{2g} w(\chi)^{2g} \\ &= w(V/F)\chi(-1)^g. \end{aligned}$$

□

References

[1] *W. Bosma*, *J. Cannon* and *C. Playoust*, The Magma algebra system. I: The user language, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[2] *T. Dokchitser* and *V. Dokchitser*, Root numbers of elliptic curves in residue characteristic 2, Bull. Lond. Math. Soc. **40** (2008), 516–524.

[3] *T. Dokchitser* and *V. Dokchitser*, Elliptic curves with all quadratic twists of positive rank, Acta Arith. **137** (2009), 193–197.

[4] *T. Dokchitser* and *V. Dokchitser*, Regulator constants and the parity conjecture, Invent. Math. **178** (2009), no. 1, 23–71.

[5] *Y. Namikawa* and *K. Ueno*, The complete classification of fibres in pencils of curves of genus two, Manuscripta Math. **9** (1973), 143–186.

[6] *M. Sabitova*, Root numbers of abelian varieties, Trans. Amer. Math. Soc. **359** (2007), no. 9, 4259–4284.

[7] *J.-P. Serre*, Abelian l-adic representations and elliptic curves, Addison-Wesley, Redwood City 1989.
[8] *J.-P. Serre* and *J. Tate*, Good reduction of abelian varieties, Ann. of Math. (2) **68** (1968), 492–517.
[9] *J. H. Silverman*, The arithmetic of elliptic curves, Grad. Texts in Math. **106**, Springer-Verlag, New York 1986.
[10] *J. H. Silverman*, Advanced topics in the arithmetic of elliptic curves, Grad. Texts in Math. **151**, Springer-Verlag, New York 1994.
[11] *W. A. Stein et al.*, Sage mathematics software (Version 4.8), The Sage Development Team, 2011, `http://www.sagemath.org`.
[12] *M. Stoll*, Rational 6-cycles under iteration of quadratic polynomials, LMS J. Comput. Math. **11** (2008), 367–380.
[13] *J. Tate*, Number theoretic background, in: Automorphic forms, representations and L-functions. Part 2 (Corvallis 1977), Proc. Sympos. Pure Math. **33**, American Mathematical Society, Providence (1979), 3–26.

Tim Dokchitser, Department of Mathematics, University Walk, Bristol BS8 1TW, United Kingdom
e-mail: tim.dokchitser@bristol.ac.uk

Vladimir Dokchitser, Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
e-mail: v.dokchitser@warwick.ac.uk

Eingegangen 8. Februar 2012